As Prepared Remarks of DNI James Clapper before the Professional Services Council Conference

Remarks as prepared for delivery by

The Honorable James R. Clapper
Director of National Intelligence

Professional Services Council Conference

Monday, October 5, 2015

The Greenbrier, White Sulfur Springs, WV

Good morning, and thank you for the invitation to kick off today's events. It's great to be here, I'm grateful for an opportunity to get away from the Beltway, even for a few hours. These days, Harry Truman's observation applies: "If you want a friend in Washington … buy a dog." Last week's political brinksmanship has become the status quo. And it isn't free. Even if we don't shut down, when we wait until the very last minute to avoid a shutdown our government and our contract workforces pay for it.

Last week, I was in a cyber-threat hearing with the Senate Armed Services Committee and NSA Director, Admiral Mike Rogers talked about all the things NSA has to do before an actual shutdown. He talked about shutting down systems, and he said that the first thing NSA has to do is cancel schools and training and pull people back from travel for training. At the end of the hearing, I spoke about the irony of a hearing on cybersecurity days before a shutdown would make us more vulnerable.

The burden on our employees for all this is ridiculous and of course, our people who are on contract are thrown into a limbo worse than our government folks. For those on our government payroll, the trend from the last few shutdowns is for Congress to go back and pay them for the time they missed. We can't do that for contracts, for contractors, or for your companies. Clearly, this is not good for our government. It's lunacy. We look ridiculous to the rest of the world.

I don't know how many meetings I've had with foreign counterparts in which they ask me to explain how our great form of government works. But we keep doing it over and over again. It reminds me of the ancient tribal wisdom that goes: "When you're riding a dead horse, the best strategy is to dismount." Well, in Washington, we sometimes do things differently.

When we find ourselves riding a dead horse, we often try strategies that are less successful

As Prepared Remarks of DNI James Clapper before the Professional Services Council Conference

such as buying a stronger whip; changing riders; saying things like, “this is the way we’ve always ridden this horse;” appointing a committee to study the horse; lowering the standards so that more dead horses can be included; appointing a tiger team to revive the dead horse; hiring outside contractors to ride the dead horse; harnessing several dead horses together to increase speed; attempting to mount multiple dead horses in hopes that one of them will spring to life; providing additional funding and training to increase the dead horse’s performance; declaring that, since a dead horse doesn’t have to be fed it’s less costly, carries lower overhead and therefore, contributes more to the mission than live horses; and my favorite, promoting the dead horse to a supervisory position.

I understand that this is just as frustrating for you as for me. From my own experience in industry in the late ‘90s, I know that your people are just as motivated by the IC’s national security mission as the government people they sit next to are. We absolutely could not do our IC mission without them, without you.

IC core-contractors help with direct technical, analytic, and administrative support to the agencies and elements. They hold the same clearances and follow precisely the same laws, policies, and regulations as government staff for access to and handling of classified information.

And we absolutely should be thinking about core contractors when we do our government workforce planning.

We’ve been increasingly tracking where we use contractors since 2007 when we first conducted an IC-wide inventory. Over the years, we’ve seen pendulum swings in how, and how much, we use core-contractors. We don’t have real data for the 1990s, not like we do now, but we know the IC, like the rest of the federal government, downsized and then outsourced a lot of our specialized skills, particularly IT.

And so after 9/11, we found that we lacked and needed people with unique skills in areas like terrorism analysis, critical languages, and cyber. So we began hiring more government staff, and while our government workforce developed those critical, unique skills we surged with professional service contractors to fill those gaps.

We also used contractors for new mission areas that we knew were limited in duration, rather than hire new permanent staff for temporary work. So we dropped contract support and government staff in the 1990s, then we surged contract support in the 2000s, after 9/11. And over the past few years, as IC needs have changed and in response to Congressional direction, the leadership of the IC has moved to rebalance the workforce, depending on fewer core

As Prepared Remarks of DNI James Clapper before the Professional Services Council Conference

contractors. This is all based on “needs.”

The direction we get seems to assume there’s a “right number” of contractors to have in the IC. There isn’t. Those are decisions that the IC leadership needs to make for their components.

In my past, I directed DIA and NGA and so, I recognize that having an oversight element tell directors what number to hit is not helpful. Dictating from “on high” how agencies use their resources is pretty much the opposite of “intell integration;” something I don’t want to do to our IC leadership. But, every year I get direction from the Hill to reduce our contractors, which we have since 2007, from about 30% of our total workforce to around 17% now.

I talk a lot about integration. It’s been my mantra for the past 5-plus years I’ve been DNI. “Integration” can be confused with “micromanagement” if you’re not careful. Integration is about bringing all the components to the table, getting them to recognize and understand their own strengths and weaknesses, their unique tradecraft, and that of the rest of the team and then getting them to work together. And of course, we have to include the attributes of the contract workforce.

I say this publicly all the time, including at last week’s testimony, we absolutely cannot meet our mission without contract support.

And by the way, to set one rumor aside, the fact that one IT system administrator stole our secrets, ran to China, released the secrets into the wild, and then ran to Russia, Russia and China: bastions of free speech and civil liberties by the way, that fact is not going to change the way we look at our core contractors.

That was an individual problem, not something related to a class of people. He could just as easily have been a government employee. So I know the question everyone here would like answered is, where are we headed with contract support? While I don’t have the clairvoyance to precisely know, I can read tea leaves, and Congressional language, well enough to see that overall resources are going to continue down. And that we’ll continue with political brinksmanship and uncertainty, which makes planning difficult.

At the same time, I can see that there are skill sets we need filled by your industry and your people. For example, we need people with STEM skills and expert technical tradecraft because keeping up with what’s on the cutting edge requires our partnership. We still need help with IT systems, but different skills than what we’ve asked for before. And we still need experts in certain mission areas. Cyber in particular is a growing mission need.

As Prepared Remarks of DNI James Clapper before the Professional Services Council Conference

So we still need your help. The numbers and the specific skill sets have fluctuated over the years, but the fundamental, symbiotic relationship between government and the professional services industry has not changed.

So, thank you for your patriotism, and for what you do for our IC and our nation. I want to save some time to have a conversation about what's on your mind, but before I go to Q&A, I want to cover four topics that industry asks me about the most often, transparency, IC ITE, cyber, and clearance reform. So indulge me for another few minutes as I do some quick hits on those topics, and then I'll give you a chance to talk.

First: Transparency. My dad was in the Signals Intelligence business in WWII. I grew up on intell sites and antenna farms all over the world and so, I already had an idea of what the intell business was about. One thing I learned for sure, we didn't discuss SIGINT at all. So my memory of not talking about the intell business goes back a long way.

For that reason, our move to transparency over the past 6 or 7 years, since our President called for a more open government, and particularly over the past 3 years or so, since the American public has decided they're going to discuss our work, whether we participate or not, has felt almost "genetically antithetical."

But one of my major takeaways of the past few years has been that, yes we have to protect our secrets: our sources and methods, our tradecraft, but we have to be more transparent about the things we can talk about because now, the American public expects us to talk about how we're using the power of U.S. intell responsibly.

That's a reason why I'm out speaking in public much more often. It's why we sent our National Intelligence Council to the South by Southwest festival this year. It's why we've published more than 5,000 pages of documents on social media and have reached millions of people with them.

And it's why just a couple weeks ago, I was in Austin, Texas at LBJ's Presidential library when we declassified 2,500 documents, President's Daily Briefings, from President Johnson's administration and from President Kennedy's.

The PDB is the absolute apex of intell reporting. It's the IC's daily dialogue with the President for addressing global challenges and opportunities related to national security. It's among the most highly classified and sensitive documents in all of government. And I don't think any other nation on the planet would declassify historical documents like those.

As Prepared Remarks of DNI James Clapper before the Professional Services Council Conference

We judged that they won't impact our current tradecraft and that they'll help the public understand what we do. So we declassified them. And we're looking for more opportunities to talk about what we're doing now. I think that will be good for our IC and our nation.

Second topic: IC ITE. For those who don't know the acronym it's the IC – IT – Enterprise, I-C-I-T-E, and we pronounce it "Eyesight." This is our effort to integrate all of the agencies' IT systems and networks into one enterprise for the whole IC.

We've finished laying the foundations for IC ITE and already, it has already made us better integrated and more secure. We've migrated millions of records into "the cloud," either the government cloud run by NSA, or the commercial cloud run by CIA. We've got tens-of-thousands of users on the common desktop and we've got a security coordination center that monitors activity across the enterprise to hopefully see anomalous behavior before someone has the chance to gather and steal as much as Snowden did.

So IC ITE is real. Even for those of us who aren't on the common desktop yet, our online identities and the secure websites we use are all managed through IC ITE shared services. So, what we need from you now is to move "up the stack," beyond system admins and even engineers, to data scientists and expert analysts who can bridge the IT-analytic gap. People who can look at the entirety of the IT enterprise, beyond data management to data governance and stewardship. If you can bring that to the table, we've got a spot for you.

My third topic is Cyber. Clearly, cyber is a pressing national security challenge. For the past three years, it has led the IC's assessment of national security threats, ever since it bumped terrorism off the top.

Cyber threats to U.S. national and economic security are increasing in frequency, scale, sophistication, and severity of impact. And, although we have to be prepared for a large, "Armageddon-scale" strike that would debilitate the entire U.S. infrastructure, our primary concern is the huge volume of low-to-moderate level cyber intrusions occurring around the clock, which will continue and probably expand, imposing increasing costs, to our businesses, to our national economic competitiveness, and to our national security.

I don't have to tell this room just how much the U.S. depends on the internet to do business. So, nearly all info communication technologies and IT networks and systems will be perpetually at risk.

Cyber espionage, criminals and terrorist entities online all undermine data "confidentiality." We can't trust that our information is private. Denial-of-service operations and data-deletion

As Prepared Remarks of DNI James Clapper before the Professional Services Council Conference

undermine “availability.” And, in the future, I believe we’ll also see more cyber operations that will change or manipulate electronic information … to compromise its “integrity.”

In other words, to compromise its accuracy and reliability, instead of deleting or disrupting access to it. And, as illustrated by the OPM breaches, counterintelligence risks are inherent when foreign intell agencies obtain access to an individual’s identification information.

So, the cyber threats to U.S. national and economic security have become increasingly diverse, sophisticated and harmful.

There are a variety of federal entities that work this cyber problem in DHS, FBI, NSA, and other law enforcement, intell, and sector specific agencies, like Treasury and Energy. Every day, these centers and entities get better at what they do individually. And the President has directed me to form a small center to integrate cyber threat intelligence. But we’re also counting on you to take simple, necessary steps to protect your information.

I’ve been out preaching the cybersecurity gospel for the past year, and this past spring I was surprised to find an online article with the headline: “What Law Firms Can Learn from James Clapper.” Most of the time, I’m on the “learning” side of the conversation when I’m talking with my attorneys. So I was curious.

Turns out, the writer was an attorney who’d caught one of my cyber discussions and had pulled out the 4 major cyber-security points I’d been pushing, which are of course, the four things our cyber experts told me to push. So by popular demand, I give the “Four Commandments of Cybersecurity” every time I talk about cyber. Here they are.

One: Patch IT software obsessively. Most cyber intrusions are through well-known vulnerabilities of commonly-used software, which can be fixed with patches already available.

Two: Segment your data. A single breach shouldn’t give attackers access to an entire network infrastructure and a mother lode of proprietary data. If you’ve seen James Cameron’s movie, Titanic, and I guess statistically, everyone here has seen it six times, you’ll remember the forensic reconstruction of the sinking; how the ship had segmented bulkheads, so that if the hull was breached, the flooding would stay isolated to just one section and the ship would stay afloat.

The forensic analysis in the film showed how the bulkheads didn’t go high enough, and so the water spilled over the top of each section into the next section until the entire ship was flooded.

As Prepared Remarks of DNI James Clapper before the Professional Services Council Conference

We tell the private sector: don't let that happen to your data. Make sure a single breach won't sink your entire company, your entire enterprise.

Cyber Commandment Three: Stay updated on the threat bulletins that DHS and FBI put out.

We regularly warn about the intrusions taking place against U.S. businesses, and we advise the private sector about how to protect itself.

And Four: Teach folks, not just your clients and your staff, but also your friends and family, what spear phishing looks like. So many times, bad actors get access to our systems and our information just by pretending to be someone else and then asking people to open an attachment or click on a link.

I'm sure those are four things everyone here already knows but there's a good reason I'm saying them again: because bad cyber actors are using precisely those avenues to steal our lunch every day. The Chinese in particular have cleaned us out because we know we're supposed to do those simple things, and yet we don't do them.

Of course, following those four commandments won't eliminate all risk and uncertainty that comes with using cyber for communication and commerce, but it will have an immediate positive impact on your vulnerabilities.

Speaking of "mitigating vulnerabilities," my fourth and last topic is clearance reform. Our current clearance system is broken and the breaches and contract service issues at OPM have only made things worse. There is, I think, light at the end of the tunnel: Continuous Evaluation.

I had the chance to get a demo of the CE program a couple weeks ago and I was blown away. The demo shows the strength of working in the cloud and improved quality of data. When this is fully in place we'll have continuous insight into the information we use for background investigations, like arrests, financial difficulties, or foreign contacts, in near-real-time, instead of every 5 years and we can get help to people who need it, before a personal problem translates into something much worse.

Implementation of a standard CE process, across the executive branch, will have a huge impact on our security clearance process. That includes better info sharing, better trust and reciprocity and better quality of data. That's a big deal to your workforces as well as ours. And it means employees also will have greater freedom of movement between contract work and government employment.

As Prepared Remarks of DNI James Clapper before the Professional Services Council Conference

My grandson joined the IC recently and he's a lot more interested in the technology than he is in committing to a company or a government agency for the next 30 years. That's a very common trait in the youngest segment of our workforce. So, we in government have to recognize and plan for our people to be mobile.

So, I want to stop there, and take some questions. Thanks again for the invitation to talk and for listening.